



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10312459 A**(43) Date of publication of application: **24 . 11 . 98**

(51) Int. Cl.

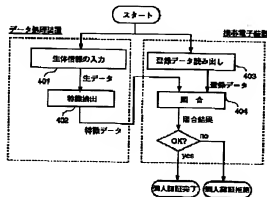
**G06T 7/00**(21) Application number: **10060815**(22) Date of filing: **12 . 03 . 98**(30) Priority: **13 . 03 . 97 JP 09 58795**(71) Applicant: **HITACHI LTD**(72) Inventor: **OKI MASARU  
SAKAGUCHI TAKAHIRO  
SATOU KAZUYASU**(54) **PORTABLE ELECTRONIC DEVICE AND  
PERSONAL AUTHENTICATION METHOD IN  
WHICH BIOLOGICAL INFORMATION IS USED**

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a personal authentication method with high security by using biological information which is impossible to be stolen or imitated.

**SOLUTION:** Characteristic volume of the biological information is stored as registration data in a portable electronic device (IC card). A user inputs one's biological information in a data processor (IC card terminal, etc.) (401). The characteristic volume is extracted regarding the inputted biological information (402) and transmitted to the portable electronic device by the data processor. The personal authentication is performed by collating characteristic data inputted from the data processor with the registration data in the portable electronic device.

COPYRIGHT: (C)1998,JPO



(51) Int.Cl.<sup>4</sup>  
G 0 6 T 7/00

識別記号

F I  
G 0 6 F 15/62

4 6 0

審査請求 未請求 請求項の畧24 O L (全 14 頁)

(21) 出願番号 特願平10-60815

(22) 出願日 平成10年(1998) 3月12日

(31) 優先権主張番号 特願平9-58795

(32) 優先日 平 9 (1997) 3月13日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 大木 良

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(72) 発明者 坂口 隆宏

東京都国分寺市東恋ヶ窪三丁目 1 番地 1

日立超エル・エス・アイ・エンジニアリング株式会社内

(72) 発明者 佐藤 和恭

茨城県土浦市神立町502番地 株式会社日立製作所機械研究所内

(74) 代理人 弁理士 小川 勝男

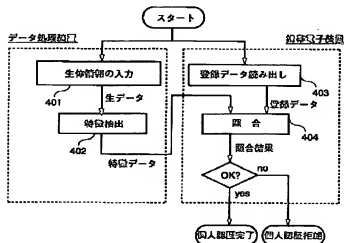
(54) 【発明の名称】 携帯電子装置及び生体情報を用いた個人認証方法

(57) 【要約】

【課題】 盗難や模倣が不可能な生体情報を用いて、セキュリティの高い個人認証方法を提供する。

【解決手段】 携帯電子装置 (ICカード) には生体情報の特徴量を登録データとして格納しておく。使用者は、自分の生体情報をデータ処理装置 (ICカードターミナル等) に入力する (401) と、データ処理装置は、入力された生体情報について特徴量を抽出して (402)、携帯電子装置に送信する。携帯電子装置ではデータ処理装置より入力された特徴データと登録データとを照合する (404) ことにより個人認証を行う。

図 4



## 【特許請求の範囲】

【請求項1】 第一の生体情報の特徴量を登録データとして記憶するメモリと、データ処理装置から認証の対象となる第二の生体情報の特徴量を特徴データとして受信する送受信インタフェースと、上記登録データと上記特徴データとを比較照合するプロセッサとを有することを特徴とする携帯電子装置。

【請求項2】 請求項1記載の携帯電子装置において、上記携帯電子装置は耐タンパ性装置であることを特徴とする携帯電子装置。

【請求項3】 請求項1記載の携帯電子装置において、上記生体情報は、指紋、網膜パターン、音声、筆跡のいずれかであることを特徴とする携帯電子装置。

【請求項4】 第一の生体情報の特徴量を登録データとして保持する携帯電子装置の個人認証を行うデータ処理装置において、

デジタル信号に変換された第二の生体情報を生データとして受信する第一の送受信インタフェースと、上記生データから特徴量を抽出するプロセッサと、上記抽出された特徴量を上記第二の生体情報の特徴データとして上記携帯電子装置に送信する第二の送受信インタフェースとを有することを特徴とするデータ処理装置。

【請求項5】 第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記データ処理装置は、入力された第二の生体情報から特徴量を抽出し、上記抽出した特徴量を特徴データとして上記携帯電子装置に送信し、

上記携帯電子装置は、上記特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項6】 第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データを上記部分登録データにより正規化し、上記正規化された特徴データを上記携帯電子装置に送信し、

上記携帯電子装置は、上記正規化された特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項7】 請求項6記載の個人認証方法において、上記データ処理装置は、上記特徴データから上記部分登録データにより、上記携帯電子装置に保持された上記登録データに相当する部分を切り出し、上記正規化された特徴データとして上記切り出された特徴データを上記携

帯電子装置に送信することを特徴とする個人認証方法。

【請求項8】 第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データと上記部分登録データとにより、上記特徴データと上記携帯電子装置に保持された登録データとの位置合わせを行い、上記特徴データと上記位置合わせについての情報とを上記携帯電子装置に送信し、  
上記携帯電子装置は、上記位置合わせについての情報に基づき、上記特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項9】 請求項8記載の個人認証方法において、上記データ処理装置は、上記位置合わせにより、上記特徴データから上記携帯電子装置に保持された上記登録データに相当する部分を切り出し、上記切り出された特徴データを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項10】 請求項8記載の個人認証方法において、上記データ処理装置は、上記特徴データと上記部分登録データとにより第一の照合処理を行い、上記特徴データと上記第一の照合処理結果とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記第一の照合処理結果に基づき、上記特徴データと上記登録データのうち上記部分登録データを除いた部分とにより第二の照合処理を行うことを特徴とする個人認証方法。

【請求項11】 請求項10記載の個人認証方法において、

上記照合処理は、上記登録データ  $A_i$  ( $1 \leq i \leq n$ ) のいずれかと上記特徴データ  $X_j$  ( $1 \leq j \leq m$ ) のいずれかの組合せの距離  $d_{ij}$  ( $1 \leq i \leq n$ ,  $1 \leq j \leq m$ ) の累積距離  $D$  の最小値と所定の閾値との比較により行い、  
上記第一の照合処理において計算対象とする上記部分登録データ  $A_i$  ( $1 \leq i \leq u$ ) と上記特徴データ  $X_j$  との組合せの範囲は、上記第二の照合処理において計算対象とする上記登録データのうち上記部分登録データを除いた部分  $A_i$  ( $u+1 \leq i \leq n$ ) と上記特徴データ  $X_j$  との組合せの範囲よりも広く設定されていることを特徴とする個人認証方法。

【請求項12】 請求項10記載の個人認証方法において、

上記生体情報は、音声または筆跡であることを特徴とする個人認証方法。

【請求項13】 第一の生体情報の特徴量を登録データと

して保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データについて所定の複数の近傍との距離を算出し、上記特徴データと上記算出された距離とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記登録データと一致する上記複数の近傍のいずれかを選択し、上記選択された近傍と上記特徴データとの距離を用いることにより、上記特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項14】請求項13記載の個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、上記特徴データと上記部分登録データとにより、上記特徴データと上記携帯電子装置に保持された登録データとの位置合わせを行い、上記特徴データと上記位置合わせについての情報とを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項15】請求項14記載の個人認証方法において、

上記データ処理装置は、上記位置合わせについての情報に基づき、上記携帯電子装置に保持された登録データに相当する部分の特徴データについて所定の複数の近傍との距離を算出し、上記特徴データと上記算出された距離とを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項16】請求項14記載の個人認証方法において、

上記データ処理装置は、上記特徴データと上記部分登録データとにより第一の照合処理を行い、上記特徴データと上記第一の照合処理結果とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記第一の照合処理結果に基づき、上記登録データのうち上記部分登録データを除いた部分について、上記登録データの部分と一致する上記複数の近傍のいずれかを選択し、上記選択された近傍と上記特徴データとの距離を用いることにより、第二の照合処理を行うことを特徴とする個人認証方法。

【請求項17】第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データを上記携帯電子装置に送信し、

上記携帯電子装置は、上記特徴データと上記登録データの差データを算出し、上記算出した差データを暗号化処理して上記データ処理装置に送信し、

上記データ処理装置は、上記暗号化された差データに基づき上記特徴データと上記登録データとについて前照合を行い、上記前照合結果を上記携帯電子装置に送信し、上記携帯電子装置は、上記前照合結果を復号し、後照合を行うことを特徴とする個人認証方法。

【請求項18】請求項17記載の個人認証方法において、

上記携帯電子装置は発生させた乱数により、上記差データをスクランブルして上記データ処理装置に送信し、上記乱数により上記データ処理装置より送信された上記前照合結果を復号することを特徴とする個人認証方法。

【請求項19】請求項17記載の個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、上記特徴データと上記部分登録データとにより、上記特徴データと上記携帯電子装置に保持された登録データとの位置合わせを行い、上記特徴データと上記位置合わせについての情報とを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項20】請求項19記載の個人認証方法において、

上記データ処理装置は、上記位置合わせにより、上記特徴データから上記携帯電子装置に保持された上記登録データに相当する部分を切り出し、上記切り出された特徴データを上記携帯電子装置に送信し、

上記携帯電子装置は、上記切り出された特徴データと上記登録データの差データを算出することを特徴とする個人認証方法。

【請求項21】請求項19記載の個人認証方法において、

上記データ処理装置は、上記特徴データと上記部分登録データとにより第一の照合処理を行い、上記特徴データと上記第一の照合処理結果とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記第一の照合処理結果に基づき、上記登録データのうち上記部分登録データを除いた部分と上記特徴データとの差データを算出し、上記算出した差データを暗号化処理して上記データ処理装置に送信し、

上記データ処理装置は、上記暗号化された差データに基づき上記特徴データと上記登録データとについて第二の照合処理における前照合を行い、上記前照合結果を上記携帯電子装置に送信し、

上記携帯電子装置は、上記前照合結果を復号し、第二の照合処理における後照合を行うことを特徴とする個人認

証方法。

【請求項22】第一の生体情報の特徴量を登録データとして保持する携帯電子装置と外部情報処理装置とネットワークにより接続されたデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、上記携帯電子装置は、上記データ処理装置より第二の生体情報の特徴量を特徴データとして入力を受け、上記登録データと上記特徴データとを照合し、上記照合の結果に基づき、個人認証の成否を判断し、

上記個人認証が成功した場合には、上記携帯電子装置は上記外部情報処理装置から暗号化されて送信される第一の情報を受信し、

上記携帯電子装置は、上記受信した第一の情報に所定の処理に必要な第二の情報を付加して暗号化し、上記外部情報処理装置に送信することを特徴とする個人認証方法。

【請求項23】請求項22記載の個人認証方法において、

上記外部処理装置は、上記携帯電子装置から送信された情報を復号し、上記第一の情報が、上記外部処理装置が上記携帯電子装置に送信した第一の情報と一致していることを条件に、上記所定の処理を実行することを特徴とする個人認証方法。

【請求項24】請求項22記載の個人認証方法において、

上記外部処理装置は、上記第一の情報として現在時刻を送信することを特徴とする個人認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード等を代表とする携帯電子装置の個人認証やインターネットなどのネットワークを通じた個人認証や電子署名に関する。例えば、第三者が不正に使用することが出来ない安全な電子通貨や、キャッシュレスショッピング、オンラインショッピング、ホームバンキング等の電子商取引に利用できる。

【0002】

【従来の技術】現在、銀行の預金引き下ろしや商品の購入において特定の個人を認証するため、情報を記憶する磁気ストライプを有するカード（以下、磁気カードと呼ぶ）が広く用いられている。キャッシュカードにより銀行の自動預け払い機から現金を引き出す場合には、暗証番号により個人認証を行う。クレジットカードにより商品購入する場合には、クレジットカード裏面の署名と商品購入時の署名とを照合し、個人認証を行っている。

【0003】このような個人認証方法には、セキュリティに関する問題点が指摘されている。キャッシュカードとその暗証番号とが第三者に盗まれた場合、容易に第三者によって預金引き出されてしまう。クレジットカードは、第三者が署名を真似ることで盗用されることもあ

(4)

る。

【0004】そこで、磁気カードに代えてICカードを使用することにより、カードに格納できる情報量を増大することに着目し、指紋や網膜パターンあるいは音声等の生体情報を使用して個人認証する方法が提案されている。これらの提案の多くは、生体情報を利用する個人認証には相当の処理負荷を要するため、ICカードターミナルで処理することが想定されている。しかし、かかる処理もまた、個人登録データが外部に流出すること、ICカードターミナルに対しては比較的容易に認証プログラムの第三者の改変が可能であることにより、セキュリティ上の問題がある。

【0005】そこで、特開昭61-199162号公報「個人識別システム」には、暗証コードとして指紋を用い、指紋の特徴抽出及び照合処理をICカードで行うアイデアが提案されている。しかしながら、ICカードのデータ処理性能は、生体情報を利用する個人認証を行うには著しく不足し、実質的に実現できないものであった。

【0006】さらに、インターネット上で商取引、選挙が行われる場合など、個人認証とともにインターネットを通じて信用情報がやり取りされる。この場合には信用情報を暗号化することにより、セキュリティを高めているが、送られてきた信用情報が本当に本人の情報であつて、リアルタイムに送られてきたかどうかを判断することは困難であつた。

【0007】

【発明が解決しようとする課題】本発明の第一の目的は、情報の記憶量が磁気カードに比べて格段に大きい携帯電子装置と盗難や模倣が困難な生体情報により個人認証を行うシステムであつて、特に、携帯電子装置に格納された生体情報を外部に流出させないことによりセキュリティを高めた個人認証システムを提供することにある。

【0008】本発明の第二の目的は、生体情報が再構成できないように処理されたデータを用いて、データ処理装置と携帯電子装置とで協調して個人認証を行うことにより、悪意のある第三者がデータ処理装置を不法に操作してシステムへ不法にアクセスすることを防止する、セキュリティの高い個人認証システムを提供することにある。

【0009】さらに、本発明の第三の目的は、外部ネットワークを通じて携帯電子装置から送られた情報が個人認証を受け、かつ、決められた時間以内に送られた情報であることを証明できるセキュリティの高い個人認証システムを提供することにある。

【0010】

【課題を解決するための手段】本発明の携帯電子装置は、第一の生体情報の特徴量を登録データとして記憶するメモリと、データ処理装置から認証の対象となる第二

10

20

30

40

50

の生体情報の特徴量を特徴データとして受信する送受信インタフェースと、登録データと特徴データとを比較照合するプロセッサとを有する。

【0011】また、本発明の生体情報を用いた個人認証方法では、データ処理装置は、入力された生体情報から特徴量を抽出し、抽出した特徴量を特徴データとして携帯電子装置に送信し、携帯電子装置は、特徴データとメモリに記憶されている生体情報の特徴量である登録データとを照合する。さらに、携帯電子装置は照合処理の一部をデータ処理装置により実行することにより、ハードウェア負荷を軽減する。

【0012】

【発明の実施の形態】図1に、ICカード等に代表される携帯電子装置の構成を示す。携帯電子装置10は、携帯電子装置10全体の制御を行うCPU102と、アプリケーションプログラムやデータを格納するRAM/ROM103と、携帯電子装置10と外部との通信を行うI/O101とを備える。RAM/ROM103はEEPROM(Electronic Erasable Programmable Read Only Memory)により構成することができ、またデータの書き換えも可能なものである。CPU102とRAM/ROM103とはアドレスバス104で、CPU101とRAM/ROM103とI/O101とは制御信号データ信号バス105で接続されている。CPU102は、外部からのI/O信号をI/O101経由で受け、RAM/ROM103上のアプリケーションプログラムを実行し、実行結果をRAM/ROM103に書き込む、あるいはI/O101経由で外部に出力する。

【0013】携帯電子装置10は1チップの中にハードウェア(101~105)及びソフトウェア(RAM/ROM)を封じ込める、あるいは携帯電子装置に対してユーザが一定の操作を加えるとソフトウェアを消去する機能を設けることにより耐タンパ性を実現した装置である。耐タンパ性装置はユーザによるソフトウェアの改竄を防止する機能を備えることにより、本発明の適用される電子商取引等の分野に使用する携帯電子装置として望ましいものである。

【0014】図2に、ICカードターミナルやICカードリーダー等に代表されるデータ処理装置20の構成を示す。データ処理装置20は、プログラムを実行するCPU201と、実行すべきプログラムやデータを格納されているRAM205と、初期プログラムブート用のROM202と、携帯電子装置と情報のやり取りを行う携帯電子装置I/O203と、外部ネットワークと情報のやり取りを行う外部I/O204と、データ処理装置20に接続される入力装置(キーボードやピンパッド等)208と出力装置(ディスプレイやスピーカ等)209を制御するユーザI/O206とを有しており、上記各構成要素はバス207により接続されている。

【0015】図3に示すように、データ処理装置20はI/O信号で携帯電子装置10と接続される。また、データ処理装置20は、必要に応じて、インターネット等のネットワークを通じて、外部情報処理装置30と情報のやり取りを行うことが出来るものである。

【0016】ここで、ICカード等に代表される携帯電子装置内のCPUやRAM/ROMは、ハードウェアをコンパクトに実現するため、また電源供給や放熱による制約から、データ処理装置(ICカードターミナルやICカードリーダー等)内のCPUやRAM/ROMに比べて、一般的に性能が劣る。

【0017】(実施例1)図4に本発明に係る個人認証システムの第1の実施例のフローチャートを示す。本実施例での処理は携帯電子装置10及びデータ処理装置20で実行される処理を含む。

【0018】データ処理装置20に、指紋や網膜パターンあるいは音声、筆跡等の生体情報が入力装置208から入力される(ステップ401)。入力された生体データの特徴をCPU201で抽出処理し(ステップ402)、抽出処理して得た特徴データを携帯電子装置10に送る。

【0019】携帯電子装置10では、登録データが格納されているRAM/ROM103から登録データを読み出し(ステップ403)、データ処理装置20から送られてきた特徴データと登録データとをCPU102で比較照合する(ステップ404)。照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【0020】本実施例での処理によれば、携帯電子装置に登録された生体情報(登録データ)を外部(データ処理装置等)に出力することなく、かつ、処理量の大きい生体情報(生データ)の特徴抽出処理をCPU性能の大きいデータ処理装置で実行するために、安全にかつ高速に個人認証を実現できる。

【0021】ここで、生体情報として指紋を使用する場合の登録データの携帯電子装置への登録方法について説明する。指紋の登録は図2に示したデータ処理装置で行われる。

【0022】図9に示したように、指紋を入力する入力装置208は、光学装置(例えば、CCDカメラ等を用いた指紋センサ)901と光学装置901から取り込まれた画像データをデジタル化するデジタル装置902とを有する。デジタル化された画像データ(生データ)はデータ処理装置20に入力される。CPU201は、生体情報の照合を容易にするために入力された生データから特徴データを抽出するプログラムを実行する。特徴を抽出する方式は様々な提案されており、これにより本発明は制約されない。例えば、南他「指紋照合のための新しいセキュリティシステム開発」(エレクトロニクス昭和

63年9月号)に記載された方法が使用できる。この方法は、図10に示すように、生データに対して階調変換(ステップ1001)、平準化(ステップ1002)、隆線方向抽出(ステップ1003)の各処理を順に施す。指紋パターンの一例を図11に示し、詳細に述べる。

【0023】階調変換1001は、生データ1101の階調(いわゆる色数)を落とす処理である。例えば256色の生データを32色に階調を落とす。平準化1002は、指紋データには、その画像の性質上、急激な階調変化は少なく、かつ隣接画素間の相関が強いことから、孤立点の除去を行う処理である。これらの処理を行った画像を格子状領域に区分し、各格子状領域における隆線方向を抽出する。各格子状領域について抽出された隆線方向パターンを特徴データ1102とする。

【0024】通常、得られた特徴データ1102の周辺領域は、入力装置の光学的歪みなどでノイズが多く含まれている。また、照合に有用な指紋の特徴位置は隆線変化の多い特徴データの中心領域である。そこで、特徴データの中心位置が多く含まれる中心領域を切り出し、切り出された部分特徴データ1103は携帯電子装置10に送る。携帯電子装置10は、部分特徴データ1103を登録データとしてRAM/ROM103に格納する。

【0025】(実施例2)図5に、本発明に係る個人認証システムの第2の実施例のフローチャートを示す。本実施例では、第1の実施例における携帯電子装置の処理の一部をデータ処理装置で行うことにより、携帯電子装置上の処理の負荷を軽減する。

【0026】データ処理装置20に生体情報が入力装置208から入力され(ステップ501)、入力された生データの特徴をCPU201で抽出処理し、特徴データを得る(ステップ502)。携帯電子装置10は、RAM/ROM103から格納されている登録データを読み出し(ステップ505)、読み出した登録データの一部分を切り出し(ステップ506)、切り出した部分登録データをデータ処理装置20に送る。

【0027】データ処理装置20では、特徴データと携帯電子装置より送られた部分登録データとから切り出し制御信号を生成し(ステップ503)、特徴データを切り出し(ステップ504)、携帯電子装置10に送る。携帯電子装置10では、切り出した特徴データと登録データとをCPU102で比較照合し(ステップ507)、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【0028】第2の実施例における認証処理をより詳細に説明する。予め登録されている登録データと認証の対象として入力された生体情報の特徴データとを照合するためには、(a)登録データと特徴データの正規化処理(指紋を生体情報とする場合には位置合わせ等の処理)

と(b)登録データと特徴データの比較処理、の2つの処理が必要である。第2の実施例では正規化処理はデータ処理装置20で行い、比較処理は携帯電子装置10で行う。携帯電子装置10では登録データから正規化処理に必要な最低限の部分登録データを抽出する。そして、正規化済み(位置合わせ済み)の特徴データを携帯電子装置10に送り、携帯電子装置10で比較処理を行う。これにより、愿意の第三者が携帯電子装置より出力された部分登録データを入力し、別の携帯電子装置にその部分登録データを登録しても、個人認証はできない。

【0029】図12に示す指紋データを例に取り、第2の実施例における比較処理の流れを詳細に説明する。認証の対象となる指紋の画像データ1204が、入力装置208からデータ処理装置20に入力され、特徴抽出処理が実行されることにより特徴データ1205を得る。

【0030】一方、携帯電子装置10では、登録データ1201を読み出し、位置合わせ用の部分登録データ1202を作成する。図12には、部分登録データ1202として登録データ1201の四隅を切り出す例を示している。位置合わせ用部分登録データ1302は登録データの盗用につながらない限り任意でよい。したがって、指紋の特徴情報を多く含まない登録データの周縁部を切り出すことが望ましく、また、照合するデータの回転を考慮して複数箇所を切り出すことが望ましい。

【0031】切り出した部分登録データ1202はデータ処理装置20に送られる。データ処理装置20は、特徴データ1205と送られてきた部分登録データ1202とから切り出し制御信号を生成する。切り出し制御信号とは、登録データ1203に一致する特徴データ1205の部分を指示する信号であり、例えば登録データ1301の四隅に対応する座標で表される。データ処理装置20は切り出し制御信号にしたがって特徴データ1205に切り出し処理を行う。これにより、4つの箇所からなる位置合わせ用データ1202を四隅とする矩形(切り出された特徴データ1206)が切り出される。

【0032】切り出された特徴データ1206は、携帯電子装置10に送られ、登録データ1203と比較照合される。

【0033】第2の実施例では、携帯電子装置に格納された生体情報の登録データと携帯電子装置の外に出力することなく、また、処理量の大きい正規化処理をCPU性能の大きいデータ処理装置により実行するために、安全、かつ高速な個人認証が実現できる。

【0034】(実施例3)図6に、本発明に係る個人認証システムの第3の実施例のフローチャートを示す。

【0035】データ処理装置20に生体情報が入力装置208から入力され(ステップ601)、入力された生データの特徴をCPU201で抽出処理し、特徴データを得る(ステップ602)。携帯電子装置10は、RAM/ROM103から格納されている登録データを読み

出し(ステップ606)、読み出した登録データの一部分を切り出し(ステップ607)、切り出した部分登録データをデータ処理装置20に送る。

【0036】データ処理装置20では、特徴データと携帯電子装置より送られた部分登録データとから切り出し制御信号を生成し(ステップ603)、特徴データを切り出す(ステップ604)。切り出された特徴データに見込み処理を行い(ステップ605)、切り出された特徴データ及び見込み処理データを携帯電子装置10に送る。携帯電子装置10では、切り出された特徴データ、見込み処理データ、登録データとをCPU102で比較照合し(ステップ608)、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【0037】生体情報として指紋を使用する場合を例として第3の実施例をより詳細に説明する。

【0038】照合処理には(a)正規化処理、(b)比較処理の2つの処理が含まれることは第2の実施例で説明したとおりである。本実施例ではさらに、比較処理における携帯電子装置の処理負担を軽減する。登録データと特徴データの比較は、両者の距離を計算し、距離の大小から判定するのが一般的である。ここで、距離の関数によつては演算量が多くなり、ハードウェア性能が貧弱な携帯電子装置にとって処理負担が大きくなる場合がある。

【0039】本実施例では、もし認証されるべき入力データが本人のものである場合には入力データは登録データの近傍に位置するという点に着目し、切り出された特徴データを近傍の範囲内でずらし、見込み距離を計算する。

【0040】図13に具体例を示す。単純化のため、特徴データを構成する隣接方向ベクトルはx軸との角度を $\alpha^\circ$ とする単位ベクトルで表示されるものと、特徴データを $a$ で代表させる。ここで、切り出された特徴データ1301が、(41、33、18、37、22、5、24、12、3)であったとする。

【0041】データ処理装置20は、例えば、最初の特徴データ「41」について、その近傍として「-2、-1、0、+1、+2」をとり、その絶対値「2、1、0、1、2」を求める。各特徴データについて許容できる近傍の範囲について予め計算した結果が見込み処理データ1302である。

【0042】携帯電子装置10では、見込み処理データ1302を受け、最初の特徴データ「41」とこれに対応した近傍データ「2、1、0、1、2」を基に、仮に登録データ列が、(40、35、20、37、20、8、28、10、5)の場合、最初の登録データが「40」なので、特徴データ「41」と比較し、差が「-1」なので、見込み処理データ「2、1、0、1、2」

から「1」を得る。同様に、次々との登録データと切り出された特徴データとを比較し、対応した見込み処理データから距離を得て、累積加算する。累積加算した結果が、登録データと切り出された特徴データとの差となり、この値が、ある閾値より小さければ、登録データと切り出された特徴データとが一致していると判断する。

【0043】以上のように、携帯電子装置10では、計算量の必要な距離計算を行わず、データ処理装置20で演算を行い、登録データと切り出された特徴データとを比較することにより、見込み処理データからテーブルlookup的に距離を得て、照合処理を行う。

【0044】なお、ここでは、1次元の特徴データを例に説明したが、次元数が増えた場合、また、距離の関数にどのようなものを用いても、携帯電子装置10の演算負担を軽減することができる。

【0045】(実施例4) 図7に、本発明に係る個人認証システムの第4の実施例のフローチャートを示す。

【0046】データ処理装置20に生体情報が入力装置208から入力され、入力された生体データの特徴をCPU201で抽出処理し、特徴データを得る。携帯電子装置10は、RAM/ROM103から格納されている登録データを読み出す。データ処理装置でのステップ701~704の処理、携帯電子装置でのステップ706、707の処理は実施例2、3と同様である。本実施例では、登録データと送られてきた特徴データとの差分を計算する(ステップ709)。この差分データに対して、ステップ708で発生させた乱数により暗号化処理を行い(ステップ710)、暗号化データをデータ処理装置20に送る。

【0047】データ処理装置20では、特徴データと送られた暗号化データで前照合処理を行い(ステップ705)、前照合データを携帯電子装置10に送る。携帯電子装置10では、前照合データと発生した乱数から後照合処理を行い(ステップ711)、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【0048】生体情報として指紋を使用する場合を例として第4の実施例をより詳細に説明する。

【0049】本実施例も第3の実施例と同様に、比較処理における携帯電子装置の処理負担を軽減することを目的とするものである。本実施例も距離を求める演算をデータ処理装置で行い、その演算結果を携帯電子装置で受け、最終照合処理を行う。

【0050】携帯電子装置10では、図14に示すように、特徴抽出された特徴データ1401と登録データ1402の差データ1403を求める。完全に特徴データの隣接方向ベクトルと登録データの隣接方向ベクトルとが一致すれば結果はゼロベクトルになるが、一般に特徴データには誤差が多く含まれるのでゼロにはならない。



ここで、この差データ1403をそのままデータ処理装置に送ると、登録データ1402が逆算されてしまう。そこで、差データ1403を乱数を使用してスクランブル(データの順序をランダムに並びかえる)し、暗号化データ1404としてデータ処理装置に送る。これにより、登録データの逆算を防止できる。

【0051】データ処理装置20では携帯電子装置10で生成された暗号化されたデータの絶対値(角度の差の絶対値を距離とする)を求め、携帯電子装置10に送る。携帯電子装置10では距離計算結果を受け、累積加算する。累積加算結果が登録データと切り出された特徴データとの差となり、この値を閾値と比較し(後照合)、閾値より小さければ、登録データと切り出された特徴データとが一致すると判断する。

【0052】単純化のため、データとして1次元の角度を使用する例で説明したが、2次元データ(例えば、ベクトル終点の座標)等多次元データを使用することももちろん可能である。また、差データを乱数でスクランブルする場合、スクランブルした結果が登録データと同じ次元であると、データ処理装置20からゼロベクトルや単位ベクトルを繰り返し送ることで、登録データが推論されるおそれがある。そこで、スクランブルにあたっては、暗号化されたデータに乱数で次元数を増やすことにより、推論を困難にすることができ。

【0053】また、本実施例では正規化処理をデータ処理装置に行っているが、携帯電子装置のハードウェア性能によっては特徴データをそのまま携帯電子装置に送信し、正規化処理及び差分処理を行わせることも可能である。

【0054】(実施例5)図8に、本発明に係る個人認証システムの第5の実施例のフローチャートを示す。本実施例は、データ処理装置が外部ネットワークと接続された環境においてセキュリティの高い個人認証システムを実現する。本実施例では、データ処理装置20はインターネット等のネットワークに接続され、ネットワークにはコンピュータ等の外部情報処理装置30(例えば、サービス提供者のホストコンピュータ)が接続されている。

【0055】データ処理装置20に生体情報が入力装置208から入力され(ステップ801)、入力された生データの特徴をCPU201で抽出処理し、特徴データを得(ステップ802)、携帯電子装置10に送る。携帯電子装置10は、RAM/ROM103から格納されている登録データを読み出し(ステップ804)、登録データと送られてきた特徴データと照合し(ステップ805)、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。以上の照合処理には、上述した第1乃至第4の実施例が適用できる。

【0056】ここで、データ処理装置20にユーザにより電子商取引に於ける金銭や取引要求等の情報が入力される。データ処理装置20は、入力された情報を読み出し(ステップ803)、携帯電子装置10に送る。ユーザによるデータ処理装置への情報の入力もしくは携帯電子装置での個人認証の完了をトリガーとして、外部情報処理装置30は現在時刻を読み出し(ステップ808)、暗号処理(ステップ809)を施し、ネットワーク経由で携帯電子装置10に送る。携帯電子装置10では、送られてきた暗号化された時刻を解読し(ステップ807)、所望の情報と送られてきた時刻とに暗号化処理を施し(ステップ806)、データ処理装置20を通り、ネットワーク経由で外部情報処理装置30に送る。外部情報処理装置30では、暗号を解読し(ステップ810)、送られてきた時刻が、自分自身が送信した時刻と一致していれば(ステップ811)、送られてきた情報が正しい情報であると判断して、所望の情報処理、例えば、電子商取引を行う(ステップ812)。

【0057】本実施例の個人認証システムは、外部情報処理装置30の指示を受け、データ処理装置からの情報を外部情報処理装置30に転送する場合に、転送処理を行う者が携帯電子装置10に登録された者(本人)であることを、外部情報処理装置30が認識するシステムである。すなわち、本発明による個人認証により第三者が携帯電子装置を悪用して登録された者に成りすますことを防ぎ、かつ、外部情報処理装置30から送られる時刻を携帯電子装置10が情報に付加して送り返すことで、データ処理装置20による改竄を防止する。

【0058】これにより、携帯電子装置10に登録された者(本人)がその時刻においてネットワークの向こうに存在していることを証明することができる。このような特性を利用すれば、一定の時間内に処理を行うことを要求されるネットワーク上で競り、選挙に有効なシステムを提供することが可能になる。

【0059】なお、データ処理装置から必要な情報が送られる例について説明したが、携帯電子装置に登録されている情報、既にデータ処理装置に格納されている情報であっても同様の処理が行える。また、外部情報処理装置において現在時刻の読み出し(ステップ808)を行うタイミングがシステムが任意に定めることができる。さらに、外部情報処理装置から現在時刻を携帯電子装置に送信するようにしているが、特に一定の時間内に処理を行うことが要求されない場合には、時刻に代えて、乱数を送るようにしても同様の効果が達成できる。

【0060】以上、実施例1から5について詳細に説明した。本発明で使用する生体情報を指紋を例として説明してきたが、勿論、指紋以外でも、2次元平面に展開できる生体情報、例えば、網膜パターンや手相、人相等、更に筆跡や声紋等のベクトル表現可能なデータ等でも入力処理を変え、特徴抽出のアルゴリズムを変えら

けで本発明を実施できる。生体情報と音声とする場合の認証(話者照合)方法について図15から図18により説明する。

【0061】図15に話者照合のフローチャートを示す。音声を入力し(ステップ1501)、入力された音声を音韻に変える(音韻処理、ステップ1502)。音韻は音声の特徴量であって、音声のスペクトル解析を基にする。このスペクトル解析による音韻処理としては、中川聖一「確率モデルによる音声認識」第10頁～第12頁(電子情報通信学会発行)に記載のLPCケプストラム分析を使用することができる。この音韻処理1502の後、音韻処理した音声に対してベクトル量子化処理を行う(ステップ1503)。音声の特徴量をベクトル量子化することにより、効率的な計算ができるようになる。このような処理1502及び1503が生体情報として音声を用いる場合の特徴抽出処理に相当する。また、携帯電子装置10にはベクトル量子化された音声の特徴量が登録データとして登録され、データ処理装置20に入力された音声の特徴データと照合される。図16に示すように、音声の特徴量は特徴ベクトルの時系列としてされ、登録データは $(A_1, A_2, \dots, A_n)$ 、入力音声の特徴データは $(X_1, X_2, \dots, X_n)$ とする。

【0062】照合処理(ステップ1504)には、DP(Dynamic Programming) マッチング法やHMM(Hidden Markov Model)法が用いられる。DPマッチング法による照合処理を、図17を用いて説明する。音声は時間的に伸縮するため時間的な変化を許容する照合が必要となる。DPマッチング法では、 $A_i$ と $X_j$ との累積距離が最小とする組合せ $(A_i, X_j)$  ( $1 \leq i \leq n, 1 \leq j \leq m$ )の時系列を求め、その場合の累積距離と所定の基準とを比較することにより照合する。

【0063】このようにDPマッチング法では、何通りの組合せの時系列について累積距離を計算する必要があるため、計算量を削減することを目的として組合せを一定の範囲に制限することが行われる。この一定の範囲を整合窓と呼ばれ、図17の直線1703と直線1704の間にあるような組合せについての累積距離の計算を行う。

【0064】まず、 $(A_i, X_j)$  ( $1 \leq j \leq r$ )の距離を比較し、距離の小さいM個の組合せ候補を抽出し、次に、このM個の候補に対して次時点での組合せ $(A_i, X_j)$ の距離と累積距離を計算し、候補を絞り込む。このような処理を繰り返す。最終的には、組合せ $(A_i, X_j)$ の時系列の中で累積距離を最小とするもの、例えば $(A_1, X_1)$ 、 $(A_1, X_2)$ 、 $(A_2, X_1)$ 、 $(A_2, X_2)$ 、 $(A_3, X_1)$ 、 $(A_3, X_2)$ 、 $(A_3, X_3)$ 、 $(A_4, X_1)$ 、 $(A_4, X_2)$ 、 $(A_4, X_3)$ 、 $(A_4, X_4)$ 、 $(A_5, X_1)$ 、 $(A_5, X_2)$ 、 $(A_5, X_3)$ 、 $(A_5, X_4)$ 、 $(A_5, X_5)$ が抽出される。このようなDPマッチング法の詳細については森健一「パターン認識」(電子情報通信学会発行)第117頁から第119頁に記載されている。

【0065】このように、話者照合においても、組合せの時系列についての累積距離の計算の処理負荷が大きく、携帯電子端末での処理は困難である。そこで、一般に発声の最初においては特徴データに変動が多い一方、発声の途中からは変動が少なくなることから、最初においては整合窓を大きくする必要があるが、途中からは整合窓を比較的に小さくしていても照合可能である点に着目する。すなわち、発声の前半の照合処理をデータ処理装置で行い(実施例5の「切り出し処理」に対応するものである)、発声の後半の照合処理を携帯電子装置で行う。前半の照合処理のため、登録データが一部分が携帯電子装置からデータ処理装置に送られるが、それ以外の部分は外部に流出することはない。

【0066】図18を用いて具体的に説明する。携帯電子装置は登録データ $A_i$  ( $1 \leq i \leq u$ )をデータ処理装置に送り、特徴データと照合する。その照合範囲は矩形1810に示された範囲となる。この場合の整合窓は広く、直線1811と直線1812によって挟まれる範囲である。携帯電子装置には照合範囲1810での照合結果が送られ、携帯電子装置では引き続き $A_i$  ( $u+1 \leq i \leq n$ )について照合処理が行われる。携帯電子装置での照合範囲は矩形1820に示された範囲となり、照合範囲1820の整合窓は直線1821と直線1822によって挟まれる範囲である。このように、携帯電子装置における照合処理では、データ処理装置における照合処理におけるよりも整合窓を狭くして計算負荷を軽減することができる。

【0067】さらに、上述した実施例3、4に対応する処理を行い、携帯電子装置において計算量を軽減することができる。実施例3に対応して、特徴データ $X_i$ の近傍 $Y_i$  ( $1 \leq k \leq 1$ )との距離を求めたものを見込み処理データとする。 $A_i$ と一致する $Y_i$ を選択し、見込み処理として予め算出した $(Y_i, X_j)$ の距離を $(A_i, X_j)$ の距離とすることができる。このようにして累積距離を最小とする組合せ $(A_i, X_j)$ の時系列を得ることができる。

【0068】また、実施例4に対応して差分処理として、組合せ $(A_i, X_j)$ の差を整合窓を満たす時系列としてとり、それに暗号処理を施して前照合処理として組合せ $(A_i, X_j)$ の距離計算を行うことができる。この場合、後照合処理として得られた累積距離からその値を最小とするものを選び、閾値と照合する。

【0069】このような特徴ベクトル列のマッチング方法は筆跡の照合にも有効なものである。

#### 【0070】

【発明の効果】本発明により、携帯電子装置に格納された生体情報を外部に流出させないことによりセキュリティを高めた個人認証システムが実現される。

【図面の簡単な説明】

【図1】携帯電子装置の構成を示す図である。

【図2】データ処理装置の構成を示す図である。

【図3】携帯電子装置とデータ処理装置と外部情報処理装置との関係を示す図である。

【図4】本発明に係る個人認証処理の第1の実施例を示す図である。

【図5】本発明に係る個人認証処理の第2の実施例を示す図である。

【図6】本発明に係る個人認証処理の第3の実施例を示す図である。

【図7】本発明に係る個人認証処理の第4の実施例を示す図である。

【図8】本発明に係る個人認証処理の第5の実施例を示す図である。

【図9】生体情報として指紋を用いる場合の入力装置の構成を示す図である。

【図10】指紋の特徴データを求める方法を示す図である。

【図11】指紋の登録データを作成する方法を示す図である。

【図12】位置合わせ用データにより位置合わせを行い、登録データと特徴データとを照合する方法を示す図である。

\* 【図13】登録データと特徴データとを照合するための見込み処理を説明する図である。

【図14】登録データと特徴データから差データを求め、暗号化データを生成する図である。

【図15】生体情報として音声を用いる場合の、話者照合方法を示す図である。

【図16】生体情報として音声を用いる場合の、登録データと特徴データとを示す図である。

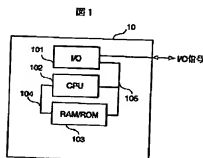
【図17】話者照合のためのDPマッチング法を示す図である。

【図18】本発明における話者照合のためのDPマッチング法を示す図である。

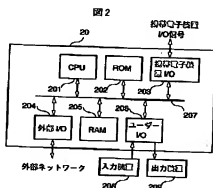
【符号の説明】

10…携帯電子装置、101…I/O(Input/Output)、102…CPU(Central Processing Unit)、103…RAM/ROM(Random Access Memory/ Read Only Memory)、104…アドレスバス、105…制御信号・データ信号バス、20…データ処理装置、201…CPU、202…ROM、203…携帯電子装置 I/O、204…外部 I/O、205…RAM、206…ユーザ I/O、207…バス、208…入力装置、209…出力装置、30…外部情報処理装置。

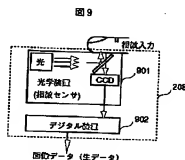
【図1】



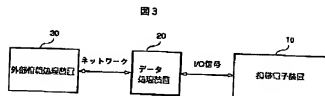
【図2】



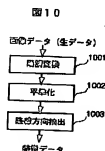
【図9】



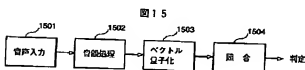
【図3】



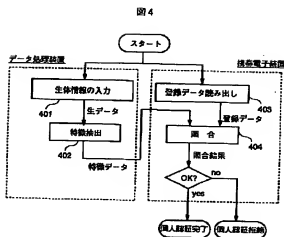
【図10】



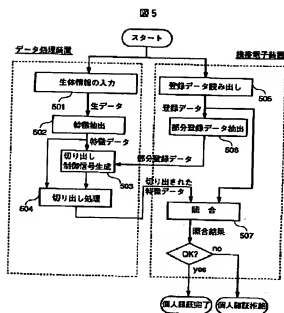
【図15】



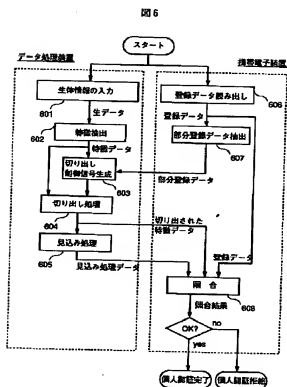
【図4】



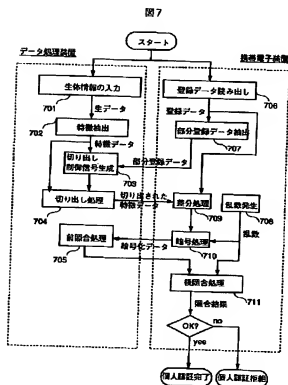
【図5】



【図6】

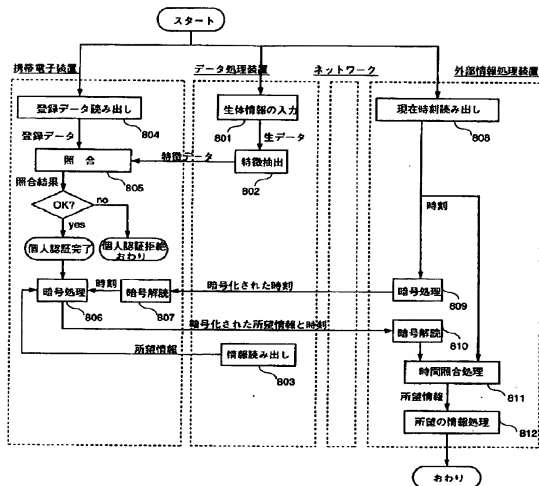


【図7】



【図8】

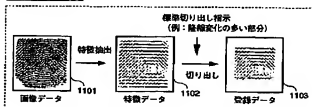
図8



【図11】

図11

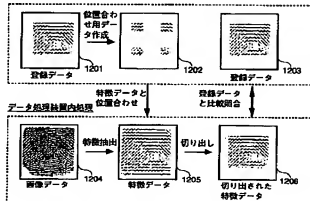
データ処理装置内処理



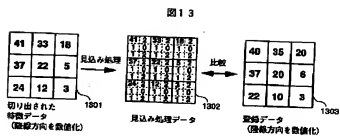
【図12】

図12

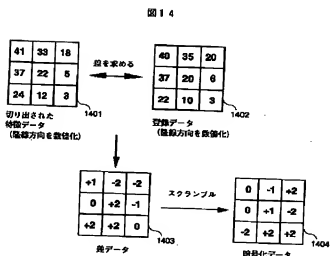
携帯電子装置内処理



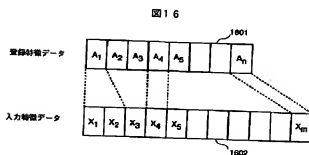
【図13】



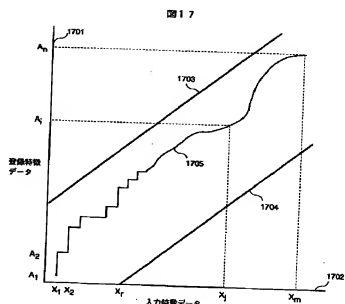
【図14】



【図16】



【図17】



【図18】

